

# On the Eschenauer-Gligor key pre-distribution scheme under on-off communication channels: The absence of isolated nodes (Extended version)

Armand M. Makowski

Department of Electrical and Computer Engineering,  
and the Institute for Systems Research, University of Maryland,  
College Park, MD 20742 USA  
E-mail: armand@isr.umd.edu.

Osman Yağan

CyLab and Department of ECE  
Carnegie Mellon University  
Moffett Field, CA 94035 USA  
Email: oyagan@ece.cmu.edu.

**Abstract**—We consider the Eschenauer-Gligor key pre-distribution scheme under the condition of partial visibility with i.i.d. on-off links between pairs of nodes. This situation is modeled as the intersection of two random graphs, namely a random key graph and an Erdős-Rényi (ER) graph. For this class of composite random graphs we give various improvements on a recent result by Yağan [17] concerning zero-one laws for the absence of isolated nodes.

**Index Terms**—Wireless sensor networks, Security, Key pre-distribution, Random graphs, Partial visibility, Absence of isolated nodes, Zero-one laws.

## I. INTRODUCTION

By now there exists already a large literature discussing various performance aspects of random key predistribution schemes in wireless sensor networks (WSNs); see [4], [12]–[15]. However, starting with the scheme of Eschenauer and Gligor [6], much of the work to date has been carried out under the *full* visibility assumption whereby sensor nodes are all within communication range of each other. While the full visibility assumption is certainly at odds with the wireless nature of the communication medium supporting WSNs, this simplification makes it possible to focus solely on how the randomization mechanism affects performance in the best of circumstances, i.e., when wireless communication is not a bottleneck. A common criticism of this line of work is that by disregarding the unreliability of the wireless links, the resulting dimensioning guidelines are likely to be overly optimistic, if not irrelevant. In practice, nodes will have fewer neighbors since some of the communication links may be impaired.

In a recent paper [17], Yağan studied the Eschenauer-Gligor key pre-distribution scheme under the condition of *partial* visibility with i.i.d. on-off links between pairs of nodes. This situation was modeled as the *intersection* of two random graphs, namely a random key graph [1], [5], [16], [18], [19], [21] and an Erdős-Rényi (ER) graph [3], [9]: With  $n$  nodes in the network, the Eschenauer-Gligor scheme with key rings of size  $K$  drawn from a pool of  $P$  distinct keys

( $K < P$ ) gives rise to the random key graph  $\mathbb{K}(n; \theta)$  (where we have set  $\theta = (K, P)$ ) – Let  $q(\theta)$  denote the probability (9) that a link does not exist between two nodes in  $\mathbb{K}(n; \theta)$ . The communication model between nodes corresponds to an Erdős-Rényi (ER) graph  $\mathbb{G}(n; \alpha)$  with link probability  $\alpha$  (in  $[0, 1]$ ). Under a natural independence assumption, the graph of interest is the graph  $\mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)$  whose edge set is the intersection of the edge sets of the random graphs  $\mathbb{K}(n; \theta)$  and  $\mathbb{G}(n; \alpha)$ . See Section II for more details concerning the model and the notation in use.

In [17] the following zero-one law for the absence of isolated nodes was established: If the parameters are scaled with the number  $n$  of nodes in such a way that

$$\alpha_n (1 - q(\theta_n)) \sim c \frac{\log n}{n} \quad (1)$$

for some  $c > 0$ , then it holds that

$$\lim_{n \rightarrow \infty} \mathbb{P} \left[ \begin{array}{c} \mathbb{K} \cap \mathbb{G}(n; \theta_n, \alpha_n) \text{ contains} \\ \text{no isolated nodes} \end{array} \right] = \begin{cases} 0 & \text{if } 0 < c < 1 \\ 1 & \text{if } 1 < c \end{cases} \quad (2)$$

provided the limit  $\lim_{n \rightarrow \infty} \alpha_n \log n$  exists in  $[0, \infty]$ .

In this short paper, we improve on this result in two different directions which are now briefly described. Precise statements are available in Section III:

(i) We show that the existence of a limit for the sequence  $\{\alpha_n \log n, n = 2, 3, \dots\}$  is not needed to ensure the zero-one law (2) under (1). In fact, this result was already contained in the earlier result of Yağan [17], and is an easy consequence of the Principle of Subsubsequences [9].

(ii) We partially strengthen the result of Yağan [17] by establishing a zero-one law when the scaling is done according to

$$\alpha_n (1 - q(\theta_n)) = \frac{\log n + \gamma_n}{n}, \quad n = 1, 2, \dots \quad (3)$$

for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ . This is done under mild conditions on the scaling  $\{\alpha_n, n = 1, 2, \dots\}$ . The class of scalings satisfying (1) is easily seen to be contained in the class of scalings governed by (3). The proof uses the method of first and second moments applied to the number of isolated nodes – This approach is presented in Section IV where expressions for the needed moments are given; see Appendix X for detailed calculations. The asymptotics of the first moment are derived in Section V in terms of a “zero-infinity” law. The bounds for applying the method of second moment are derived in Section VI. The proof of the zero-law under the scaling (3) is completed in Section VII, Section VIII and Section IX.

The material of this paper appeared in the Proceedings of the 53rd Annual Allerton Conference on Communication, Control, and Computing, Monticello (IL) [11].

## II. THE MODEL

All limiting statements, including asymptotic equivalences, are understood with the number  $n$  of sensor nodes going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple  $(\Omega, \mathcal{F}, \mathbb{P})$ . Probabilistic statements are made with respect to this probability measure  $\mathbb{P}$ , and we denote the corresponding expectation operator by  $\mathbb{E}$ . The indicator function of an event  $E$  is denoted by  $\mathbf{1}[E]$ . For any discrete set  $S$  we write  $|S|$  for its cardinality.

### A. The Eschenauer-Gligor scheme

The Eschenauer-Gligor scheme is characterized by three parameters, which are held fixed throughout this section, namely the number  $n$  of nodes, the size  $P$  of the key pool and the size  $K$  of each key ring with  $K < P$ . To lighten the notation we often group the integers  $P$  and  $K$  into the ordered pair  $\theta \equiv (K, P)$ .

Nodes are labelled  $i = 1, \dots, n$ . For each  $i = 1, \dots, n$ , let  $K_i(\theta)$  denote the random set of  $K$  distinct keys assigned to node  $i$  before network deployment. According to the Eschenauer-Gligor scheme, if after deployment, two nodes, say  $i$  and  $j$ , are within communication range of each other, they can establish a secure link provided their key rings have at least one key in common.

We can think of  $K_i(\theta)$  as an  $\mathcal{P}_K$ -valued rv where  $\mathcal{P}_K$  denotes the collection of all subsets of  $\{1, \dots, P\}$  which contain exactly  $K$  elements – Obviously, we have  $|\mathcal{P}_K| = \binom{P}{K}$ . The rvs  $K_1(\theta), \dots, K_n(\theta)$  are assumed to be *i.i.d.* rvs, each of which is *uniformly* distributed over  $\mathcal{P}_K$  with

$$\mathbb{P}[K_i(\theta) = S] = \binom{P}{K}^{-1}, \quad \begin{array}{l} i = 1, \dots, n \\ S \in \mathcal{P}_K. \end{array} \quad (4)$$

This corresponds to selecting keys randomly and *without* replacement from the key pool.

For future reference, for any subset  $R$  of  $\{1, \dots, P\}$  we find it convenient to write

$$v(\theta; R) = \begin{cases} \frac{\binom{P-|R|}{K}}{\binom{P}{K}} & \text{if } |R| \leq P - K \\ 0 & \text{if } P - K < |R|. \end{cases} \quad (5)$$

Since  $v(\theta; R)$  depends on  $R$  only through its cardinality  $|R|$ , sometimes we shall also write  $v(\theta; |R|)$  in place of  $v(\theta; R)$ . It is a simple matter to check that

$$\mathbb{P}[K_i(\theta) \cap R = \emptyset] = v(\theta; R), \quad i = 1, \dots, n. \quad (6)$$

### B. Random key graphs

Under full visibility, the Eschenauer-Gligor scheme gives rise to a random graph which we now describe: Distinct nodes  $i$  and  $j$  are said to be  $K$ -adjacent, written  $i \sim_K j$ , if their key rings have at least one key in common. Thus,

$$i \sim_K j \quad \text{iff} \quad K_i(\theta) \cap K_j(\theta) \neq \emptyset, \quad (7)$$

and an undirected link is assigned between nodes  $i$  and  $j$ . This notion of adjacency defines the *random key graph*  $\mathbb{K}(n; \theta)$  on the vertex set  $\{1, \dots, n\}$ .

For distinct  $i, j = 1, \dots, n$ , it is a simple matter to check from (6) that

$$\mathbb{P}[K_i(\theta) \cap K_j(\theta) = \emptyset] = q(\theta) \quad (8)$$

with

$$q(\theta) = \begin{cases} 0 & \text{if } P < 2K \\ \frac{\binom{P-K}{K}}{\binom{P}{K}} & \text{if } 2K \leq P. \end{cases} \quad (9)$$

Note that  $q(\theta) = v(\theta, K)$ . It is plain that

$$\mathbb{P}[i \sim_K j] = 1 - q(\theta) \quad (10)$$

so that the probability of edge occurrence between any two nodes is equal to  $1 - q(\theta)$ .

### C. ER graphs as a simple communication model

To account for the possibility that communication links between nodes may not be available, we assume a simple communication model that consists of independent communication channels, each of which can be either on or off. Thus, with  $\alpha$  in  $[0, 1]$ , let  $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$  denote i.i.d.  $\{0, 1\}$ -valued rvs with success probability  $\alpha$ . For convenience we also introduce the  $\{0, 1\}$ -valued rvs  $\{B_{ji}(\alpha), 1 \leq i < j \leq n\}$  by setting

$$B_{ji}(\alpha) = B_{ij}(\alpha), \quad 1 \leq i < j \leq n.$$

The channel between nodes  $i$  and  $j$  is available (equivalently, up) if  $B_{ij}(\alpha) = 1$  with probability  $\alpha$ , and unavailable (equivalently, down) if  $B_{ij}(\alpha) = 0$  with complementary probability  $1 - \alpha$ . Distinct nodes  $i$  and  $j$  are said to be  $B$ -adjacent, written  $i \sim_B j$ , if  $B_{ij}(\alpha) = 1$ . The notion of  $B$ -adjacency defines the standard ER graph  $\mathbb{G}(n; \alpha)$  on the vertex set  $\{1, \dots, n\}$ . Obviously,

$$\mathbb{P}[i \sim_B j] = \alpha.$$

#### D. Intersecting the graphs

The random graph model studied here is obtained by *intersecting* the random key graph  $\mathbb{K}(n; \theta)$  with the ER graph  $\mathbb{G}(n; \alpha)$ : The distinct nodes  $i$  and  $j$  are now said to be adjacent, written  $i \sim j$ , if and only if they are both K-adjacent and B-adjacent, namely

$$i \sim j \quad \text{iff} \quad \begin{array}{c} K_i(\theta) \cap K_j(\theta) \neq \emptyset \\ \text{and} \\ B_{ij}(\alpha) = 1. \end{array} \quad (11)$$

The resulting undirected random graph defined on the vertex set  $\{1, \dots, n\}$  through this notion of adjacency is denoted  $\mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)$ .

Throughout, the collections of rvs  $\{K_1(\theta), \dots, K_n(\theta)\}$  and  $\{B_{ij}(\alpha), 1 \leq i < j \leq n\}$  are assumed to be *independent*, in which case the probability of edge occurrence in  $\mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)$  is given by

$$\mathbb{P}[i \sim j] = \mathbb{P}[i \sim_K j] \mathbb{P}[i \sim_B j] = p(\theta, \alpha) \quad (12)$$

where we have set

$$p(\theta, \alpha) = \alpha(1 - q(\theta)). \quad (13)$$

Finally, to simplify the notation, we set

$$P_n(\theta, \alpha) = \mathbb{P} \left[ \begin{array}{c} \mathbb{K} \cap \mathbb{G}(n; \theta_n, \alpha_n) \text{ contains} \\ \text{no isolated nodes} \end{array} \right].$$

### III. THE MAIN RESULTS

To fix the terminology, we refer to any pair of mappings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  as a scaling (for random key graphs) provided the natural conditions

$$K_n < P_n, \quad n = 1, 2, \dots \quad (14)$$

are satisfied. Similarly, any mapping  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  defines a scaling for ER graphs.

The terminology of strong and very strong zero-one laws parallels the one introduced in the survey papers [8, Section IV, p. 1070] [10]. The first result gives a very strong one-law for the absence of isolated nodes under minimal assumptions; its proof is given in Section V.

**Theorem III.1.** *Consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that*

$$\alpha_n(1 - q(\theta_n)) = \frac{\log n + \gamma_n}{n}, \quad n = 1, 2, \dots \quad (15)$$

*for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ . The very strong one-law*

$$\lim_{n \rightarrow \infty} P_n(\theta_n, \alpha_n) = 1 \quad (16)$$

*holds whenever*

$$\lim_{n \rightarrow \infty} \gamma_n = \infty. \quad (17)$$

It is noteworthy that Theorem III.1 applies to the constant parameter case, yielding a result similar to the one available for many classes of random graphs, e.g., ER graphs [3], [9],

geometric random graphs [7] and random key graphs [20]. The proof is straightforward and is omitted in the interest of brevity.

**Corollary III.2.** *With  $\alpha$  in  $(0, 1]$  and positive integers  $K$  and  $P$  such that  $K < P$ , we always have  $\lim_{n \rightarrow \infty} P_n(\theta, \alpha) = 1$  provided  $\alpha(1 - q(\theta)) > 0$ .*

**Proof.** We can write

$$\alpha(1 - q(\theta)) = \frac{\log n + \gamma_n}{n}, \quad n = 1, 2, \dots$$

with deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$  given by

$$\gamma_n = n\alpha(1 - q(\theta)) - \log n, \quad n = 1, 2, \dots$$

The desired conclusion is a simple consequence of Theorem III.1 as we note that  $\lim_{n \rightarrow \infty} \gamma_n = \infty$  under the condition  $\alpha(1 - q(\theta)) > 0$ . ■

While no additional condition are needed in Theorem III.1, the corresponding zero-law does require growth conditions on the scaling  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$ .

**Theorem III.3.** *Consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that (15) holds for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ . The very strong zero-law*

$$\lim_{n \rightarrow \infty} P_n(\theta_n, \alpha_n) = 0 \quad (18)$$

*holds whenever*

$$\lim_{n \rightarrow \infty} \gamma_n = -\infty \quad (19)$$

*provided either*

$$\limsup_{n \rightarrow \infty} \alpha_n \log n < \infty, \quad (20)$$

*or*

$$\limsup_{n \rightarrow \infty} \alpha_n \log n = \infty \quad \text{with} \quad \limsup_{n \rightarrow \infty} \alpha_n < 1. \quad (21)$$

A proof of Theorem III.3 is developed through Sections IV to VII. The additional growth conditions (20)-(21) can be dropped when restricting attention to the scalings used by Yağan [17].

**Theorem III.4.** *Consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that*

$$\alpha_n(1 - q(\theta_n)) \sim c \frac{\log n}{n} \quad (22)$$

*for some  $c > 0$ . Then, the strong zero-one law*

$$\lim_{n \rightarrow \infty} P_n(\theta_n, \alpha_n) = \begin{cases} 0 & \text{if } 0 < c < 1 \\ 1 & \text{if } 1 < c \end{cases} \quad (23)$$

*holds.*

**Proof.** Consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow$

$[0, 1]$  such that (22) holds for some  $c > 0$ . This can be rewritten in equivalent form as

$$\alpha_n(1 - q(\theta_n)) = c_n \cdot \frac{\log n}{n}, \quad n = 1, 2, \dots \quad (24)$$

where the sequence  $c : \mathbb{N}_0 \rightarrow \mathbb{R}_+$  satisfies  $\lim_{n \rightarrow \infty} c_n = c$ . It is then plain that (15) automatically holds with deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$  given by

$$\gamma_n = (c_n - 1) \log n, \quad n = 1, 2, \dots$$

When  $c > 1$ , we have  $\lim_{n \rightarrow \infty} \gamma_n = \infty$  and Theorem III.1 gives the one-law (16), hence the one-law part of (23) holds. On the other hand, with  $0 < c < 1$ ,  $\lim_{n \rightarrow \infty} \gamma_n = -\infty$  and Theorem III.3 yields the zero-law (18), hence the zero-law part of (23), if the additional conditions (20) or (21) hold. We now show that this additional condition is superfluous for the zero-law to hold; this is a consequence of the Principle of Subsubsequences [9] – In what follows a subsequence  $k \rightarrow n_k$  is simply any non-decreasing mapping  $\mathbb{N}_0 \rightarrow \mathbb{N}_0 : k \rightarrow n_k$  such that  $\lim_{k \rightarrow \infty} n_k = \infty$ :

A careful inspection of the arguments given by Yağan [17, Thm. 3.1, p. 3824] shows that the result also holds along subsequences: Specifically, consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that (22) holds for some  $c$  in  $(0, 1)$ . Then, for any subsequence  $k \rightarrow n_k$ , we have

$$\lim_{k \rightarrow \infty} P_{n_k}(\theta_{n_k}, \alpha_{n_k}) = 0 \quad (25)$$

whenever the limit  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k$  exists in  $[0, \infty]$ .

The sequence

$$\{P_n(\theta_n, \alpha_n), \quad n = 2, 3, \dots\} \quad (26)$$

is a bounded sequence with *all* its accumulation points in  $[0, 1]$ . Let  $P$  be *any* accumulation point of the sequence. By definition, there exists a subsequence  $k \rightarrow n_k$  such that

$$\lim_{k \rightarrow \infty} P_{n_k}(\theta_{n_k}, \alpha_{n_k}) = P. \quad (27)$$

Although the sequence  $\{\alpha_{n_k} \log n_k, \quad k = 1, 2, \dots\}$  may not converge, there must exist a further subsequence  $\ell \rightarrow k_\ell$  such that the limit  $\lim_{\ell \rightarrow \infty} \alpha_{n_{k_\ell}} \log n_{k_\ell}$  does exist in  $[0, \infty]$ .

Taking (27) along that subsequence we find

$$\lim_{\ell \rightarrow \infty} P_{n_{k_\ell}}(\theta_{n_{k_\ell}}, \alpha_{n_{k_\ell}}) = P,$$

whence  $P = 0$  by virtue of (25). The *bounded* sequence (26) thus admits  $P = 0$  as its *unique* accumulation point, and is therefore convergent with limit

$$\lim_{n \rightarrow \infty} P_n(\theta_n, \alpha_n) = 0$$

regardless of whether the sequence  $\{\alpha_n \log n, \quad n = 1, 2, \dots\}$  has a limit in  $[0, \infty]$ . ■

#### IV. THE METHOD OF FIRST AND SECOND MOMENTS

Theorem III.1 and Theorem III.3 will be established by the method of first and second moments [9, p. 55] applied to the number of isolated nodes. Fix  $n = 2, 3, \dots$  and consider positive integers  $K$  and  $P$  such that  $K < P$ , and scalar  $\alpha$  in  $[0, 1]$ .

##### A. Counting isolated nodes

The number of isolated nodes in  $\mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)$  is given by

$$I_n(\theta, \alpha) = \sum_{i=1}^n \chi_{n,i}(\theta, \alpha)$$

where for each  $i = 1, 2, \dots, n$ , we write

$$\chi_{n,i}(\theta, \alpha) = \mathbf{1} [\text{Node } i \text{ is isolated in } \mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)].$$

It is a simple matter to check that

$$\chi_{n,i}(\theta, \alpha) = \prod_{j=1, j \neq i}^n (1 - B_{ij}(\alpha) \eta_{ij}(\theta)) \quad (28)$$

with indicator rvs

$$\eta_{ij}(\theta) = \mathbf{1} [K_i(\theta) \cap K_j(\theta) \neq \emptyset], \quad i, j = 1, \dots, n, \quad i \neq j \quad (29)$$

The random graph  $\mathbb{K} \cap \mathbb{G}(n; \theta, \alpha)$  has no isolated nodes if and only if  $I_n(\theta, \alpha) = 0$ , and the key relation

$$P_n(\theta, \alpha) = \mathbb{P}[I_n(\theta, \alpha) = 0]$$

follows.

This equivalence is exploited with the help of two standard bounds based on first and second moments: The easy bound

$$1 - \mathbb{E}[I_n(\theta, \alpha)] \leq \mathbb{P}[I_n(\theta, \alpha) = 0] \quad (30)$$

gives rise to the method of first moment [9, Eqn. (3.10), p. 55], while the method of second moment [9, Remark 3.1, p. 55] has its starting point in the inequality

$$\mathbb{P}[I_n(\theta, \alpha) = 0] \leq 1 - \frac{(\mathbb{E}[I_n(\theta, \alpha)])^2}{\mathbb{E}[I_n(\theta, \alpha)^2]}. \quad (31)$$

##### B. Evaluating moments

The rvs  $\chi_{n,1}(\theta, \alpha), \dots, \chi_{n,n}(\theta, \alpha)$  being exchangeable, we readily get

$$\mathbb{E}[I_n(\theta, \alpha)] = n \mathbb{E}[\chi_{n,1}(\theta, \alpha)] \quad (32)$$

and

$$\begin{aligned} \mathbb{E}[I_n(\theta, \alpha)^2] &= n \mathbb{E}[\chi_{n,1}(\theta, \alpha)] \\ &\quad + n(n-1) \mathbb{E}[\chi_{n,1}(\theta, \alpha) \chi_{n,2}(\theta, \alpha)]. \end{aligned}$$

This last expression is an easy consequence of the binary nature of the rvs involved. It then follows that

$$\begin{aligned} \frac{\mathbb{E}[I_n(\theta, \alpha)^2]}{(\mathbb{E}[I_n(\theta, \alpha)])^2} &= \frac{1}{\mathbb{E}[\chi_{n,1}(\theta, \alpha)]} \\ &\quad + \frac{n-1}{n} \cdot \frac{\mathbb{E}[\chi_{n,1}(\theta, \alpha) \chi_{n,2}(\theta, \alpha)]}{(\mathbb{E}[\chi_{n,1}(\theta, \alpha)])^2}. \end{aligned} \quad (33)$$

With (28) as point of departure, expressions are easily obtained for the needed moments  $\mathbb{E}[\chi_{n,1}(\theta, \alpha)]$  and  $\mathbb{E}[\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha)]$ ; calculations are given in Appendix X for sake of completeness: In the notation (13), we have

$$\mathbb{E}[\chi_{n,1}(\theta, \alpha)] = (1 - p(\theta, \alpha))^{n-1}, \quad (34)$$

whence

$$\mathbb{E}[I_n(\theta, \alpha)] = n(1 - p(\theta, \alpha))^{n-1}. \quad (35)$$

We also show that

$$\begin{aligned} \mathbb{E}[\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha)] \\ = \mathbb{E}[(1 - \alpha\eta_{12}(\theta))Z(\theta, \alpha)^{n-2}] \end{aligned} \quad (36)$$

where the auxiliary rv  $Z(\theta, \alpha)$  is given by

$$Z(\theta, \alpha) = (1 - p(\theta, \alpha))^2 \left(1 + \tilde{Z}(\theta, \alpha)\right) \quad (37)$$

with

$$\begin{aligned} \tilde{Z}(\theta, \alpha) \\ = \frac{\alpha^2}{(1 - p(\theta, \alpha))^2} \cdot (v(\theta; K_1(\theta) \cup K_2(\theta)) - q(\theta)^2). \end{aligned} \quad (38)$$

## V. BEHAVIOR OF THE FIRST MOMENT

The proof of Theorem III.1 passes through a characterization of the behavior of the first moment given in the following “zero-infinity” law – Note its “analogy” with Theorem III.1.

**Lemma V.1.** *Consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that (15) holds for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ . It is always the case that*

$$\lim_{n \rightarrow \infty} \mathbb{E}[I_n(\theta_n, \alpha_n)] = \begin{cases} \infty & \text{if } \lim_{n \rightarrow \infty} \gamma_n = -\infty \\ 0 & \text{if } \lim_{n \rightarrow \infty} \gamma_n = \infty. \end{cases} \quad (39)$$

Before establishing this result, we note that the proof of Theorem III.1 is now straightforward: The bound (30) yields  $\lim_{n \rightarrow \infty} \mathbb{P}[I_n(\theta_n, \alpha_n) = 0] = 1$  whenever  $\lim_{n \rightarrow \infty} \mathbb{E}[I_n(\theta_n, \alpha_n)] = 0$ , as this is the case under the condition (17) by virtue of Lemma V.1. ■

Although the proof of Lemma V.1 is fairly standard, we give some of the details as we need to develop some facts that will be used later: We start with the observation that for  $0 \leq x < 1$ ,

$$\log(1 - x) = -x - \Psi(x) \quad \text{with} \quad \Psi(x) = \int_0^x \frac{t}{1 - t} dt.$$

It is also easy to check that

$$\lim_{x \downarrow 0} \frac{\Psi(x)}{x^2} = \frac{1}{2}. \quad (40)$$

Now consider scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that (15) holds for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ .

For each  $n = 1, 2, \dots$ , substitution of (15) into (35) yields

$$\begin{aligned} \mathbb{E}[I_n(\theta_n, \alpha_n)] &= n(1 - p(\theta_n, \alpha_n))^{n-1} \\ &= ne^{(n-1)\log(1 - p(\theta_n, \alpha_n))} \\ &= ne^{-(n-1)(p(\theta_n, \alpha_n) + \Psi(p(\theta_n, \alpha_n)))} \\ &= ne^{-(n-1)\frac{\log n + \gamma_n}{n} - (n-1)\Psi(p(\theta_n, \alpha_n))} \\ &= n^{\frac{1}{n}} e^{-\frac{n-1}{n}\gamma_n} e^{-(n-1)\Psi(p(\theta_n, \alpha_n))} \end{aligned} \quad (41)$$

as well as the bound

$$\mathbb{E}[I_n(\theta_n, \alpha_n)] \leq n^{\frac{1}{n}} e^{-\frac{n-1}{n}\gamma_n}. \quad (42)$$

If  $\lim_{n \rightarrow \infty} \gamma_n = \infty$ , then  $\lim_{n \rightarrow \infty} \mathbb{E}[I_n(\theta_n, \alpha_n)] = 0$  by virtue of the inequality (42). On the other hand, the condition  $\lim_{n \rightarrow \infty} \gamma_n = -\infty$  already implies  $\lim_{n \rightarrow \infty} n^{\frac{1}{n}} e^{-\frac{n-1}{n}\gamma_n} = \infty$ . In view of (41), the desired conclusion  $\lim_{n \rightarrow \infty} \mathbb{E}[I_n(\theta_n, \alpha_n)] = \infty$  then holds if we show

$$\lim_{n \rightarrow \infty} (n-1)\Psi(p(\theta_n, \alpha_n)) = 0. \quad (43)$$

To do so, note that the condition  $\lim_{n \rightarrow \infty} \gamma_n = -\infty$  also implies  $\gamma_n < 0$  for all  $n$  sufficiently large, in which case  $\gamma_n = -|\gamma_n|$ . On that range the condition (15) becomes

$$0 \leq p(\theta_n, \alpha_n) = \frac{\log n - |\gamma_n|}{n},$$

whence

$$|\gamma_n| \leq \log n \quad \text{and} \quad p(\theta_n, \alpha_n) \leq \frac{\log n}{n}. \quad (44)$$

Therefore, we must have

$$\lim_{n \rightarrow \infty} p(\theta_n, \alpha_n) = 0 \quad (45)$$

as well as

$$\lim_{n \rightarrow \infty} (n-1)p(\theta_n, \alpha_n)^2 = 0. \quad (46)$$

The conclusion (43) is an easy consequence of these two facts (combined with (40)) once we note that

$$(n-1)\Psi(p(\theta_n, \alpha_n)) = (n-1)p(\theta_n, \alpha_n)^2 \cdot \frac{\Psi(p(\theta_n, \alpha_n))}{p(\theta_n, \alpha_n)^2}$$

for all  $n = 1, 2, \dots$  ■

## VI. BOUNDS

The proof of the zero-law relies on various bounds which we now develop. Fix  $n = 2, 3, \dots$  and consider positive integers  $K$  and  $P$  such that  $K < P$ , and scalar  $\alpha$  in  $[0, 1]$ .

By uninteresting calculations it follows from (34), (36), (37) and (38) that

$$\frac{\mathbb{E}[\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha)]}{(\mathbb{E}[\chi_{n,1}(\theta, \alpha)])^2} = (1 - p(\theta, \alpha))^{-2} \cdot R_n(\theta, \alpha) \quad (47)$$



with

$$\begin{aligned} R_n(\theta, \alpha) &= \mathbb{E} \left[ (1 - \alpha \eta_{12}(\theta)) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right] \\ &= \mathbb{E} \left[ (1 - \eta_{12}(\theta)) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right] \\ &\quad + (1 - \alpha) \mathbb{E} \left[ \eta_{12}(\theta) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right]. \end{aligned} \quad (48)$$

From the expression (5) it is plain that

$$v(\theta; 2K) \leq v(\theta; |K_1(\theta) \cup K_2(\theta)|) \leq v(\theta; K) \quad (49)$$

with the lower (resp. upper) bound corresponding to  $K_1(\theta) \cap K_2(\theta) = \emptyset$  (resp.  $K_1(\theta) = K_2(\theta)$ ).

In the first term in (48), the event  $[\eta_{12}(\theta) = 0]$  coincides with the event  $[K_1(\theta) \cap K_2(\theta) = \emptyset]$ , in which case we have  $|K_1(\theta) \cup K_2(\theta)| = 2K$  so that

$$v(\theta; K_1(\theta) \cup K_2(\theta)) - q(\theta)^2 = v(\theta; 2K) - q(\theta)^2.$$

We then conclude that

$$\begin{aligned} &\mathbb{E} \left[ (1 - \eta_{12}(\theta)) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right] \\ &= q(\theta) \left( 1 + \frac{\alpha^2 (v(\theta; 2K) - q(\theta)^2)}{(1 - p(\theta, \alpha))^2} \right)^{n-2}. \end{aligned} \quad (50)$$

It is plain that

$$\begin{aligned} &(1 - p(\theta, \alpha))^2 - \alpha^2 q(\theta)^2 \\ &= (1 - p(\theta, \alpha) - \alpha q(\theta)) (1 - p(\theta, \alpha) + \alpha q(\theta)) \\ &= (1 - \alpha) (1 - \alpha + 2\alpha q(\theta)) > 0. \end{aligned} \quad (51)$$

We also observe that

$$v(\theta; 2K) < q(\theta)^2$$

by easy calculations based on the combinatorial expressions for the quantities involved; details are left to the interested reader. As a result, we have

$$0 \leq 1 + \frac{\alpha^2 (v(\theta; 2K) - q(\theta)^2)}{(1 - p(\theta, \alpha))^2} \leq 1$$

and the conclusion

$$\mathbb{E} \left[ (1 - \eta_{12}(\theta)) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right] \leq q(\theta) \quad (52)$$

follows.

As we turn to the second term in (48), it follows from (49) that

$$\begin{aligned} \tilde{Z}(\theta, \alpha) &\leq \frac{\alpha^2 (v(\theta; K) - q(\theta)^2)}{(1 - p(\theta, \alpha))^2} \\ &= \frac{\alpha^2 (q(\theta) - q(\theta)^2)}{(1 - p(\theta, \alpha))^2} \\ &= \frac{\alpha^2 q(\theta) (1 - q(\theta))}{(1 - p(\theta, \alpha))^2}. \end{aligned} \quad (53)$$

Using this deterministic bound we obtain

$$\begin{aligned} &(1 - \alpha) \mathbb{E} \left[ \eta_{12}(\theta) \left( 1 + \tilde{Z}(\theta, \alpha) \right)^{n-2} \right] \\ &\leq (1 - \alpha) \mathbb{E} [\eta_{12}(\theta)] \left( 1 + \frac{\alpha^2 q(\theta) (1 - q(\theta))}{(1 - p(\theta, \alpha))^2} \right)^{n-2} \\ &= (1 - \alpha) (1 - q(\theta)) \left( 1 + \frac{\alpha q(\theta) p(\theta, \alpha)}{(1 - p(\theta, \alpha))^2} \right)^{n-2} \\ &\leq (1 - \alpha) (1 - q(\theta)) \cdot R_n^*(\theta, \alpha) \end{aligned} \quad (54)$$

where we have set

$$R_n^*(\theta, \alpha) = e^{(n-2) \frac{\alpha q(\theta) p(\theta, \alpha)}{(1 - p(\theta, \alpha))^2}}. \quad (55)$$

Collecting (52) and (54) we obtain the key bound

$$R_n(\theta, \alpha) \leq q(\theta) + (1 - q(\theta)) R_n^*(\theta, \alpha). \quad (56)$$

Later on we shall also have use for the quantity

$$R_n^o(\theta, \alpha) = e^{(1 - p(\theta, \alpha))^{-2} \cdot \alpha \log n}. \quad (57)$$

## VII. A PROOF OF THEOREM III.3: THE BASIC APPROACH

The proof of the zero-law of Theorem III.3 is developed in the next three sections. For the remainder of the paper, we consider fixed scalings  $K, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0$  and  $\alpha : \mathbb{N}_0 \rightarrow [0, 1]$  such that (15) holds for some deviation function  $\gamma : \mathbb{N}_0 \rightarrow \mathbb{R}$ . We also assume that (19) holds.

From (31) the zero-law  $\lim_{n \rightarrow \infty} \mathbb{P}[I_n(\theta_n, \alpha_n) = 0] = 0$  will be established if we can show that

$$\liminf_{n \rightarrow \infty} \frac{(\mathbb{E}[I_n(\theta_n, \alpha_n)])^2}{\mathbb{E}[I_n(\theta_1, \alpha_n)]^2} \geq 1. \quad (58)$$

In view of (33) this will be achieved if the limiting statements

$$\lim_{n \rightarrow \infty} \mathbb{E}[I_n(\theta_n, \alpha_n)] = \infty \quad (59)$$

and

$$\limsup_{n \rightarrow \infty} \left( \frac{\mathbb{E}[\chi_{n,1}(\theta_n, \alpha_n) \chi_{n,2}(\theta_n, \alpha_n)]}{(\mathbb{E}[\chi_{n,1}(\theta_n, \alpha_n)])^2} \right) \leq 1 \quad (60)$$

both hold.

As the former holds by virtue of Lemma V.1 under (19), it remains only to show the latter. Using (45) we conclude from (47) that establishing (60) is equivalent to showing

$$\limsup_{n \rightarrow \infty} R_n(\theta_n, \alpha_n) \leq 1, \quad (61)$$

and this will hold if we show the *stronger* inequality

$$\limsup_{n \rightarrow \infty} (q(\theta_n) + (1 - q(\theta_n)) R_n^*(\theta_n, \alpha_n)) \leq 1. \quad (62)$$

Under (15), by the remarks made in the proof of Lemma V.1, we see that the exponent in  $R_n^*(\theta_n, \alpha_n)$  satisfies

$$\begin{aligned} &(n-2) \frac{\alpha_n q(\theta_n) \cdot p(\theta_n, \alpha_n)}{(1 - p(\theta_n, \alpha_n))^2} \\ &= \frac{n-2}{n} \frac{\alpha_n q(\theta_n) \log n}{(1 - p(\theta_n, \alpha_n))^2} - \frac{n-2}{n} \frac{\alpha_n q(\theta_n) |\gamma_n|}{(1 - p(\theta_n, \alpha_n))^2} \\ &\leq (1 - p(\theta_n, \alpha_n))^{-2} \cdot \alpha_n \log n \end{aligned} \quad (63)$$

for  $n = 2, 3, \dots$  sufficiently large. On that range this leads to the bound

$$R_n^*(\theta_n, \alpha_n) \leq R_n^\circ(\theta_n, \alpha_n) \quad (64)$$

as we recall (57). Therefore, (62) will hold if we show the stronger statement

$$\limsup_{n \rightarrow \infty} (q(\theta_n) + (1 - q(\theta_n))R_n^\circ(\theta_n, \alpha_n)) \leq 1. \quad (65)$$

During the discussion we shall make use of the following two observations: First the equality

$$\begin{aligned} q(\theta_n) + (1 - q(\theta_n))R_n^\circ(\theta_n, \alpha_n) \\ = 1 + (1 - q(\theta_n))(R_n^\circ(\theta_n, \alpha_n) - 1) \end{aligned} \quad (66)$$

holds for all  $n = 1, 2, \dots$ . Next, as already noted in the proof of Lemma V.1, condition (19) yields  $\gamma_n = -|\gamma_n|$  and  $|\gamma_n| \leq \log n$  eventually. Thus, for  $n = 1, 2, \dots$  sufficiently large, whenever it happens that  $\alpha_n > 0$ , we have the bounds

$$\begin{aligned} 1 - q(\theta_n) &= \frac{1}{\alpha_n} \cdot \frac{\log n - |\gamma_n|}{n} \\ &\leq \frac{1}{\alpha_n} \cdot \frac{\log n}{n} \\ &= \frac{1}{\alpha_n \log n} \cdot \frac{(\log n)^2}{n}. \end{aligned} \quad (67)$$

### VIII. ALONG SUBSEQUENCES

Several cases need to be considered on the basis of the behavior of the sequence  $\{\alpha_n \log n, n = 1, 2, \dots\}$  along subsequences.

**Lemma VIII.1.** Assume that along the subsequence  $k \rightarrow n_k$ , the limit  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k$  exists with

$$\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k = 0. \quad (68)$$

Then, under (15) with (19) we have both

$$\lim_{k \rightarrow \infty} R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k}) = 1, \quad (69)$$

and

$$\lim_{k \rightarrow \infty} (q(\theta_{n_k}) + (1 - q(\theta_{n_k}))R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k})) = 1. \quad (70)$$

**Proof.** Under the enforced assumptions, we have

$$\lim_{k \rightarrow \infty} (1 - p(\theta_{n_k}, \alpha_{n_k}))^{-2} \cdot \alpha_{n_k} \log n_k = 0$$

as we recall (45). The conclusion (69) is then straightforward from the expression (57), and (70) follows upon using (66). ■

In this last step we had no information concerning  $\lim_{k \rightarrow \infty} q(\theta_{n_k})$ , hence the need for (66) in order to conclude (70).

**Lemma VIII.2.** Assume that along the subsequence  $k \rightarrow n_k$ , the limit  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k$  exists in  $(0, \infty)$ . Then, under (15) with (19) we have both

$$\lim_{k \rightarrow \infty} q(\theta_{n_k}) = 1 \quad (71)$$

and

$$\lim_{k \rightarrow \infty} (1 - q(\theta_{n_k})) R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k}) = 0, \quad (72)$$

whence (70) holds.

**Proof.** The condition  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k > 0$  implies  $\alpha_{n_k} > 0$  eventually. This together with condition (19) allows us to use (67) eventually along the subsequence  $k \rightarrow n_k$ . Thus, for all  $k = 1, 2, \dots$  sufficiently large, we have

$$1 - q(\theta_{n_k}) \leq \frac{1}{\alpha_{n_k} \log n_k} \cdot \left( \frac{(\log n_k)^2}{n_k} \right), \quad (73)$$

and the conclusion (71) immediately follows. Finally, using (45) we get

$$\lim_{k \rightarrow \infty} R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k}) = e^{\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k} \quad (74)$$

where the limit is finite by assumption, and the conclusion (72) follows from (71). The convergence (70) is now straightforward. ■

**Lemma VIII.3.** Assume that along the subsequence  $k \rightarrow n_k$ , the limit  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k$  exists with

$$\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k = \infty. \quad (75)$$

Then, under (15) with (19) we still have (71) whereas both (70) and (72) hold provided the additional condition

$$\limsup_{k \rightarrow \infty} \alpha_{n_k} < 1 \quad (76)$$

is enforced.

**Proof.** It is plain that (71) still holds under the condition  $\lim_{k \rightarrow \infty} \alpha_{n_k} \log n_k = \infty$  since the bound (73) is valid here as well since  $\alpha_{n_k} > 0$  eventually for all  $k = 1, 2, \dots$  sufficiently large. In order to justify (72) under the additional condition (76) we argue as follows: Consider  $k = 1, 2, \dots$  sufficiently large so that (73) holds. We have

$$\begin{aligned} (1 - q(\theta_{n_k})) R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k}) \\ \leq \frac{1}{\alpha_{n_k} \log n_k} \cdot \left( \frac{(\log n_k)^2}{n_k} \right) R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k}) \\ = \frac{1}{\alpha_{n_k} \log n_k} \cdot (\log n_k)^2 \cdot \frac{R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k})}{n_k} \end{aligned} \quad (77)$$

with

$$\begin{aligned} \frac{R_{n_k}^\circ(\theta_{n_k}, \alpha_{n_k})}{n_k} \\ = \frac{1}{n_k} \cdot e^{(1 - p(\theta_{n_k}, \alpha_{n_k}))^{-2} \cdot \alpha_{n_k} \log n_k} \\ = e^{(-1 + (1 - p(\theta_{n_k}, \alpha_{n_k}))^{-2} \cdot \alpha_{n_k}) \log n_k}. \end{aligned}$$

By virtue of (45), we find that

$$\begin{aligned} & \limsup_{k \rightarrow \infty} (-1 + (1 - p(\theta_{n_k}, \alpha_{n_k}))^{-2} \cdot \alpha_{n_k}) \\ &= -1 + \limsup_{k \rightarrow \infty} \frac{\alpha_{n_k}}{(1 - p(\theta_{n_k}, \alpha_{n_k}))^2} \\ &= -1 + \left( \limsup_{k \rightarrow \infty} \alpha_{n_k} \right) < 0, \end{aligned} \quad (78)$$

under the additional condition (76), whence

$$\lim_{k \rightarrow \infty} \left( (\log n_k)^2 \cdot \frac{R_{n_k}^o(\theta_{n_k}, \alpha_{n_k})}{n_k} \right) = 0. \quad (79)$$

Let  $k$  to infinity in (77): The validity of (72) now follows by appealing to (75) and (79). Here as well the convergence (70) is straightforward. ■

In summary, under their specific assumptions, each of Lemma VIII.1, Lemma VIII.2 and Lemma VIII.3 ensures that (70) holds, hence  $\limsup_{k \rightarrow \infty} R_{n_k}(\theta_{n_k}, \alpha_{n_k}) \leq 1$  and the conclusion

$$\lim_{k \rightarrow \infty} P_{n_k}(\theta_{n_k}, \alpha_{n_k}) = 0$$

follows.

#### IX. COMPLETING THE PROOF OF THEOREM III.3

The proof of Theorem III.3 relies on the Subsequence Principle: For any arbitrary subsequence  $k \rightarrow n_k$ , we shall show that there exists a further subsequence  $\ell \rightarrow k_\ell$  such that

$$\lim_{\ell \rightarrow \infty} P_{n_{k_\ell}}(\theta_{n_{k_\ell}}, \alpha_{n_{k_\ell}}) = 0. \quad (80)$$

It is well known that this implies  $\lim_{n \rightarrow \infty} P_n(\theta_n, \alpha_n) = 0$ .

If

$$\limsup_{n \rightarrow \infty} \alpha_n \log n < \infty,$$

then  $\limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k < \infty$  as well, and there exists a subsequence  $\ell \rightarrow k_\ell$  such that

$$\lim_{\ell \rightarrow \infty} \alpha_{n_{k_\ell}} \log n_{k_\ell} = \limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k$$

When  $\limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k = 0$ , we invoke Lemma VIII.1 (applied to the subsequence  $\ell \rightarrow n_{k_\ell}$ ) to conclude that (80) holds. On the other hand, if  $\limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k$  is an element of  $(0, \infty)$  we also conclude to (80) by appealing to Lemma VIII.2 (applied to the subsequence  $\ell \rightarrow n_{k_\ell}$ ).

If

$$\limsup_{n \rightarrow \infty} \alpha_n \log n = \infty,$$

then there are two possibilities:

(i) If  $\limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k < \infty$ , then the earlier analysis applies unchanged and leads to the existence of a subsequence  $\ell \rightarrow k_\ell$  such that (80) holds.

(ii) If  $\limsup_{k \rightarrow \infty} \alpha_{n_k} \log n_k = \infty$ , there exists at least one subsequence  $\ell \rightarrow k_\ell$  such that

$$\lim_{\ell \rightarrow \infty} \alpha_{n_{k_\ell}} \log n_{k_\ell} = \infty$$

On the other hand, the condition  $\limsup_{n \rightarrow \infty} \alpha_n < 1$  implies  $\limsup_{\ell \rightarrow \infty} \alpha_{n_{k_\ell}} < 1$ , and Lemma VIII.3 (applied to the subsequence  $\ell \rightarrow n_{k_\ell}$ ) ensures that (80) holds.

#### ACKNOWLEDGMENT

This work was supported by NSF Grant CCF-1217997. The paper was completed during the academic year 2014-2015 while A.M. Makowski was a Visiting Professor with the Department of Statistics of the Hebrew University of Jerusalem with the support of a fellowship from the Lady Davis Trust.

#### REFERENCES

- [1] S.R. Blackburn and S. Gerke, "Connectivity of the uniform random intersection graph," *Discrete Mathematics* **309** (2009), pp. 5130-5140.
- [2] M. Bloznelis, J. Jaworski and K. Rybarczyk, "Component evolution in a secure wireless sensor network," *Networks* **53** (2009), pp. 19-26.
- [3] B. Bollobás, *Random Graphs*, Second Edition, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.
- [4] S. A. Çamtepe and B. Yener, *Key Distribution Mechanisms for Wireless Sensor Networks: a Survey*, Technical Report TR-05-07, Rensselaer Polytechnic Institute, Computer Science Department, Troy (NY), March 2005.
- [5] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Transactions on Information Systems Security TISSEC* **11** (2008), pp. 1-22.
- [6] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the ACM Conference on Computer and Communications Security (CSS 2002), Washington (DC), November 2002, pp. 41-47.
- [7] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks, Chapter in *Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, Edited by W.M. McEneaney, G. Yin and Q. Zhang, Birkhauser, Boston (MA), 1998.
- [8] G. Han and A.M. Makowski, "Sensitivity of critical transmission ranges to node placement distributions," *IEEE Journal on Selected Areas in Communications JSAC-27* (2009), Special Issue on Stochastic Geometry and Random Graphs for Wireless Networks, pp. 1066-1078.
- [9] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, 2000.
- [10] A.M. Makowski and G. Han, *On the Sensitivity of the Critical Transmission Range: Lessons from the Lonely Dimension*, Foundations and Trends in Networking **6** (2011), pp. 287-399.
- [11] A.M. Makowski and O. Yağan, "On the Eschenauer-Gligor key pre-distribution scheme under on-off communication channels: The absence of isolated nodes," in Proceedings of the 53rd Annual Allerton Conference on Communication, Control, and Computing, Monticello (IL), September 2015.
- [12] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM* **47** (2004), pp. 53-57.
- [13] D.-M. Sun and B. He, "Review of key management mechanisms in wireless sensor networks," *Acta Automatica Sinica* **12** (2006), pp. 900-906.
- [14] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials* **8** (2006), pp. 2-23.
- [15] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications* **30** (2007), pp. 2314-2341.
- [16] O. Yağan, *Random Graph Modeling of Key Distribution Schemes in Wireless Sensor Networks*, Ph.D. Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park (MD), June 2011.
- [17] O. Yağan, "Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel," *IEEE Transactions on Information Theory* **IT-58** (2012), pp. 3821-3835.
- [18] O. Yağan and A.M. Makowski, "On the random graph induced by a random key predistribution scheme under full visibility," in Proceedings of the IEEE International Symposium on Information Theory (ISIT 2008), Toronto (ON), June 2008.
- [19] O. Yağan and A. M. Makowski, "Connectivity results for random key graphs," in Proceedings of the IEEE International Symposium on Information Theory (ISIT 2009), Seoul (Korea), June 2009.



- [20] O. Yağan and A.M. Makowski, “Connectivity in random graphs induced by a key predistribution scheme Small key pools,” in Proceedings of the 44th Annual Conference on Information Sciences and Systems (CISS 2010), Princeton (NJ), March 2010.
- [21] O. Yağan and A.M. Makowski, “Zero-one laws for connectivity in random key graphs,” *IEEE Transactions on Information Theory* **IT-58** (2012), pp. 2983-2999.

## X. APPENDIX: PROOF OF (34) AND (36)

Fix  $n = 2, 3, \dots$ , positive integers  $K$  and  $P$  such that  $K < P$ , and  $\alpha$  in  $[0, 1]$ . From (28) we note that

$$\chi_{n,j}(\theta, \alpha) = (1 - B_{12}(\alpha)\eta_{12}(\theta)) \cdot \prod_{\ell=3}^n (1 - B_{j\ell}(\alpha)\eta_{j\ell}(\theta))$$

for  $j = 1, 2$ .

It follows from (6) that the indicator rvs  $\eta_{12}(\theta), \dots, \eta_{1n}(\theta)$  are i.i.d.  $\{0, 1\}$  rvs, so that the rvs  $\eta_{12}(\theta), \dots, \eta_{1n}(\theta), B_{12}(\alpha), \dots, B_{1n}(\alpha)$  are mutually independent under the enforced independence assumptions. Therefore,

$$\begin{aligned} \mathbb{E}[\chi_{n,1}(\theta, \alpha)] &= \mathbb{E}\left[\prod_{\ell=2}^n (1 - B_{1\ell}(\alpha)\eta_{1\ell}(\theta))\right] \\ &= \prod_{\ell=2}^n \mathbb{E}[1 - B_{1\ell}(\alpha)\eta_{1\ell}(\theta)] \\ &= \prod_{\ell=2}^n (1 - \mathbb{E}[B_{1\ell}(\alpha)] \mathbb{E}[\eta_{1\ell}(\theta)]) \\ &= \prod_{\ell=2}^n (1 - \alpha(1 - q(\theta))), \end{aligned} \quad (81)$$

and we obtain the expression (34).

Next, we observe that

$$\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha) = (1 - B_{12}(\alpha)\eta_{12}(\theta)) \cdot (\dots)$$

with

$$\dots = \prod_{\ell=3}^n (1 - B_{1\ell}(\alpha)\eta_{1\ell}(\theta)) (1 - B_{2\ell}(\alpha)\eta_{2\ell}(\theta)).$$

Upon conditioning with respect to the rvs  $K_1(\theta), \dots, K_n(\theta)$ , we get

$$\begin{aligned} \mathbb{E}[\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha)] \\ = \mathbb{E}\left[(1 - \alpha\eta_{12}(\theta)) \cdot \prod_{\ell=3}^n (1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta))\right] \end{aligned}$$

under the enforced independence assumptions. It is also easy to check that *conditionally* on  $K_1(\theta)$  and  $K_2(\theta)$ , the  $n - 2$  pairs of rvs  $(\eta_{13}(\theta), \eta_{23}(\theta)), \dots, (\eta_{1n}(\theta), \eta_{2n}(\theta))$  are mutually independent, whence

$$\begin{aligned} \mathbb{E}\left[\prod_{\ell=3}^n (1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta)) \middle| K_1(\theta), K_2(\theta)\right] \\ = \prod_{\ell=3}^n \mathbb{E}[(1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta)) | K_1(\theta), K_2(\theta)]. \end{aligned}$$

For each  $\ell = 3, \dots, n$  and  $j = 1, 2$ , it is plain that

$$\begin{aligned} \mathbb{E}[\eta_{j\ell}(\theta) | K_1(\theta), K_2(\theta)] \\ = \mathbb{E}[\mathbf{1}[K_j(\theta) \cap K_\ell(\theta) \neq \emptyset] | K_i(\theta)] \\ = 1 - q(\theta). \end{aligned} \quad (82)$$

Therefore,

$$\begin{aligned} \mathbb{E}[(1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta)) | K_1(\theta), K_2(\theta)] \\ = 1 - 2\alpha(1 - q(\theta)) + \alpha^2 \mathbb{E}[\eta_{1\ell}(\theta)\eta_{2\ell}(\theta) | K_1(\theta), K_2(\theta)] \\ = (1 - \alpha(1 - q(\theta)))^2 \\ + \alpha^2 (\mathbb{E}[\eta_{1\ell}(\theta)\eta_{2\ell}(\theta) | K_1(\theta), K_2(\theta)] - (1 - q(\theta))^2) \end{aligned}$$

by a completion-of-square argument. With the product rv  $\eta_{1\ell}(\theta)\eta_{2\ell}(\theta)$  given by

$$\begin{aligned} (1 - \mathbf{1}[K_1(\theta) \cap K_\ell(\theta) = \emptyset]) (1 - \mathbf{1}[K_2(\theta) \cap K_\ell(\theta) = \emptyset]) \\ = 1 - \mathbf{1}[K_1(\theta) \cap K_\ell(\theta) = \emptyset] - \mathbf{1}[K_2(\theta) \cap K_\ell(\theta) = \emptyset] \\ + \mathbf{1}[K_1(\theta) \cap K_\ell(\theta) = \emptyset] \mathbf{1}[K_2(\theta) \cap K_\ell(\theta) = \emptyset] \\ = 1 - \mathbf{1}[K_1(\theta) \cap K_\ell(\theta) = \emptyset] - \mathbf{1}[K_2(\theta) \cap K_\ell(\theta) = \emptyset] \\ + \mathbf{1}[(K_1(\theta) \cup K_2(\theta)) \cap K_\ell(\theta) = \emptyset], \end{aligned}$$

it follows that

$$\begin{aligned} \mathbb{E}[\eta_{1\ell}(\theta)\eta_{2\ell}(\theta) | K_1(\theta), K_2(\theta)] \\ = 1 - 2q(\theta) + v(\theta; K_1(\theta) \cup K_2(\theta)) \end{aligned} \quad (83)$$

so that

$$\begin{aligned} \mathbb{E}[\eta_{1\ell}(\theta)\eta_{2\ell}(\theta) | K_1(\theta), K_2(\theta)] - (1 - q(\theta))^2 \\ = 1 - 2q(\theta) + v(\theta; K_1(\theta) \cup K_2(\theta)) - (1 - q(\theta))^2 \\ = v(\theta; K_1(\theta) \cup K_2(\theta)) - q(\theta)^2. \end{aligned} \quad (84)$$

Collecting terms we conclude that

$$\begin{aligned} \mathbb{E}[(1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta)) | K_1(\theta), K_2(\theta)] \\ = (1 - p(\theta, \alpha))^2 + \alpha^2 (v(\theta; K_1(\theta) \cup K_2(\theta)) - q(\theta)^2). \end{aligned}$$

Upon substitution into earlier expressions, we now obtain

$$\begin{aligned} \mathbb{E}\left[\prod_{\ell=3}^n (1 - \alpha\eta_{1\ell}(\theta)) (1 - \alpha\eta_{2\ell}(\theta)) \middle| K_1(\theta), K_2(\theta)\right] \\ = Z(\theta; \alpha)^{n-2} \end{aligned}$$

with the rv  $Z(\theta; \alpha)$  is given by

$$\begin{aligned} Z(\theta; \alpha) \\ = (1 - p(\theta, \alpha))^2 + \alpha^2 (v(\theta; K_1(\theta) \cup K_2(\theta)) - q(\theta)^2) \end{aligned} \quad (85)$$

Finally,

$$\mathbb{E}[\chi_{n,1}(\theta, \alpha)\chi_{n,2}(\theta, \alpha)] = \mathbb{E}[(1 - \alpha\eta_{12}(\theta)) Z(\theta; \alpha)^{n-2}].$$

and we note that the rv  $Z(\theta; \alpha)$  given at (85) coincides with the rv given through the expressions (37)-(38). ■